

The best possible upper bound on the probability of undetected error for linear codes of full support

Torleiv Kløve and Jinquan Luo, Department of Informatics, University of Bergen, N-5020 Bergen, Norway

Abstract—There is a known best possible upper bound on the probability of undetected error for linear codes. The $[n, k; q]$ codes with probability of undetected error meeting the bound have support of size k only. In this note, linear codes of full support ($= n$) are studied. A best possible upper bound on the probability of undetected error for such codes is given, and the codes with probability of undetected error meeting this bound are characterized.

UPPER BOUNDS ON $P_{\text{ue}}(C, p)$ FOR LINEAR CODES C

Let $n \geq k \geq 1$. An $[n, k; q]$ code is a linear code of length n and dimension k over the field F_q of q elements.

For an $[n, k; q]$ code C , the probability of undetected error $P_{\text{ue}}(C, p)$ is the probability that a codeword is changed to another codeword when transmitted over the q -ary symmetric channel. It is known, see [1, Theorem 2.51], that

Theorem 1: If C is an $[n, k; q]$ code, then

$$P_{\text{ue}}(C, p) \leq (1-p)^{n-k} - (1-p)^n \quad (1)$$

for all $p \in [0, (q-1)/q]$. Moreover, the bound is best possible since the bound is met with equality for all p for the code $C_{n,k}$ generated by $[I_k | 0_{k \times (n-k)}]$. Here I_k is the $k \times k$ identity matrix, and $0_{k \times (n-k)}$ is the $k \times (n-k)$ matrix with all entries zero.

It is known (see e.g. [1] Theorem 2.1) that

$$P_{\text{ue}}(C, p) = (1-p)^n \left\{ A_C \left(\frac{p}{(q-1)(1-p)} \right) - 1 \right\}$$

where $A_C(z)$ is the weight distribution function of C . In terms of the weight distribution, (1) is equivalent to

$$A_C(z) \leq A_{C_{n,k}}(z) \text{ for all } z \in [0, 1].$$

For a code C of length n , the support $\chi(C)$ is the set of positions i such that $c_i \neq 0$ for some codeword $(c_1, c_2, \dots, c_n) \in C$. The code has *full support* if $|\chi(C)| = n$, that is, for any position there is a codeword that is non-zero in this position. For example, the code $C_{n,k}$ has support k .

In practical applications, one usually uses codes with full support. We expect to find a sharper upper bound on $P_{\text{ue}}(C, p)$ for codes of full support. In this paper we find the following best possible upper bound on $P_{\text{ue}}(C, p)$ for linear codes of full support.

Theorem 2: If C is an $[n, k; q]$ code of full support, then

$$P_{\text{ue}}(C, p) \leq (1-p)^{n-k+1} + (q-1)^{k-n} p^{n-k+1} - (1-p)^n$$

for all $p \in [0, (q-1)/q]$. Moreover, the bound is best possible since the bound is met with equality for all p for the code

$D_{n,k,\mathbf{v}}$ generated by

$$\begin{bmatrix} I_k & \mathbf{v} \\ 0_{(k-1) \times (n-k)} & \end{bmatrix},$$

where $\mathbf{v} \in F_q^{n-k}$ is a vector of full support (that is, without zero in any position). Moreover, any code of full support meeting the bound is equivalent to $D_{n,k,\mathbf{v}}$ for some \mathbf{v} of full support.

This bound is tighter than the bound (1). The improvement for $p \in (0, (q-1)/q)$ is

$$p(1-p)^{n-k} \left\{ 1 - \left(\frac{p}{(q-1)(1-p)} \right)^{n-k} \right\}.$$

PROOF OF THEOREM 2

The weight distribution of $D_{n,k,\mathbf{v}}$ is

$$A_{D_{n,k,\mathbf{v}}}(z) = (1 + (q-1)z)^{k-1} (1 + (q-1)z^{n-k+1}).$$

Therefore, Theorem 2 is equivalent to

Theorem 3: If C is an $[n, k; q]$ code of full support, then

$$A_C(z) \leq (1 + (q-1)z)^{k-1} (1 + (q-1)z^{n-k+1})$$

for all $z \in [0, 1]$, with equality if and only if C is equivalent to $D_{n,k,\mathbf{v}}$ for some vector \mathbf{v} of full support.

Lemma 1: An $[n, k; q]$ code C has full support if and only if C^\perp is an $[n, k, 2; q]$ code, that is, it has minimum distance at least 2.

Proof: The result follows from the observation that if i is not in the support, then the unit vector \mathbf{e}_i is contained in C^\perp and vice versa. ■

By the MacWilliams theorem, if C is an $[n, k; q]$ code, then

$$A_{C^\perp}(z) = \frac{1}{q^k} (1 + (q-1)z)^n A_C \left(\frac{1-z}{1 + (q-1)z} \right). \quad (2)$$

This implies that $A_{C_1}(z) \leq A_{C_2}(z)$ for all $z \in [0, 1]$ if and only if $A_{C_1^\perp}(z) \leq A_{C_2^\perp}(z)$ for all $z \in [0, 1]$.

Let $E_{n,k,\mathbf{v}} = D_{n,n-k,\mathbf{v}}^\perp$. This code is generated by the matrix $[I_k | \mathbf{v}^t | 0_{k \times (n-k-1)}]$.

Using (2), we see that

$$A_{E_{n,n-k,\mathbf{v}}}(z) = \frac{1}{q} \left\{ (1 + (q-1)z)^{n-k+1} + (q-1)(1-z)^{n-k+1} \right\}. \quad (3)$$

Combining all these facts, we see that Theorem 3 is equivalent to the following (where we substitute $n-k$ for k).

Theorem 4: If C is an $[n, k, 2; q]$ code, then

$$A_C(z) \leq f(z), \quad (4)$$

where

$$f(z) = \frac{1}{q} \left\{ (1 + (q-1)z)^{k+1} + (q-1)(1-z)^{k+1} \right\},$$

for all $z \in [0, 1]$, with equality if and only if C is equivalent to $E_{n,k,\mathbf{v}}$ for some vector $\mathbf{v} \in F_q^k$ of full support.

Before proving this theorem, we give a couple of simple lemmas. For $z \in [0, 1]$ we clearly have $z^i \geq z^j$ for $i \leq j$. This implies the following lemma.

Lemma 2: For $[n, k; q]$ codes C and C' , if

$$\sum_{i=1}^j A_i(C) \leq \sum_{i=1}^j A_i(C')$$

for any $1 \leq j \leq n$, then for all $z \in [0, 1]$, we have

$$A_C(z) \leq A_{C'}(z).$$

Moreover, we have equality for any $z \in (0, 1)$ if and only if $A_i(C) = A_i(C')$ for all i , $1 \leq i \leq n$.

Lemma 3: Let \mathbf{v} be a vector of full support. Then

a)

$$A_i(E_{n,k,\mathbf{v}}) = \frac{1}{q} \binom{k+1}{i} \{ (q-1)^i + (q-1)(-1)^i \}.$$

b)

$$\begin{aligned} \sum_{i=2}^j A_i(E_{n,k,\mathbf{v}}) &= \sum_{i=1}^{j-1} \binom{k}{i} (q-1)^i \\ &+ \frac{1}{q} \binom{k}{j} \{ (q-1)^j + (-1)^j (q-1) \}. \end{aligned} \quad (5)$$

Proof: We see that a) follows immediately from (3). From

a) we get

$$\begin{aligned} \sum_{i=2}^j A_i(E_{n,k,\mathbf{v}}) &= \frac{1}{q} \sum_{i=2}^j \binom{k+1}{i} (q-1)^i \\ &+ \frac{q-1}{q} \sum_{i=2}^j \binom{k+1}{i} (-1)^i. \end{aligned}$$

Let

$$F(z) = \sum_{i=2}^j \binom{k+1}{i} z^i.$$

Then

$$\begin{aligned} F(z) &= \sum_{i=2}^j \binom{k}{i} z^i + \sum_{i=2}^j \binom{k}{i-1} z^i \\ &= \sum_{i=2}^j \binom{k}{i} z^i + \sum_{i=1}^{j-1} \binom{k}{i} z^{i+1} \\ &= (z+1) \sum_{i=1}^{j-1} \binom{k}{i} z^i + \binom{k}{j} z^j - zk. \end{aligned}$$

Hence

$$\begin{aligned} q \sum_{i=2}^j A_i(E_{n,k,\mathbf{v}}) &= F(q-1) + (q-1)F(-1) \\ &= q \sum_{i=1}^{j-1} \binom{k}{i} (q-1)^i + \binom{k}{j} (q-1)^j - (q-1)k \\ &\quad + (q-1) \binom{k}{j} (-1)^j + (q-1)k. \end{aligned}$$

Hence, b) follows. ■

We now give the proof of Theorem 4.

Proof: Suppose C is generated by $G = [I_k | Q]$ where the rows of Q are $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k$ (and where $\mathbf{v}_i \neq \mathbf{0}$ for $1 \leq i \leq k$). Then for any $\mathbf{x} \in F_q^k$, the codeword $\mathbf{x}G = (\mathbf{x} | \mathbf{x}Q)$ has weight

$$w(\mathbf{x}G) = w(\mathbf{x}) + w(\mathbf{x}Q).$$

Hence

$$\sum_{i=2}^j A_i(C) = S_1 + S_2, \quad (6)$$

where

$$\begin{aligned} S_1 &= |\{ \mathbf{x} \mid \mathbf{x} \neq \mathbf{0}, w(\mathbf{x}) \leq j-1, w(\mathbf{x}Q) + w(\mathbf{x}) \leq j \}| \\ &\leq |\{ \mathbf{x} \mid \mathbf{x} \neq \mathbf{0}, w(\mathbf{x}) \leq j-1 \}| \\ &= \sum_{i=1}^{j-1} \binom{k}{i} (q-1)^i, \end{aligned}$$

and

$$S_2 = |\{ \mathbf{x} \mid w(\mathbf{x}) = j, \mathbf{x}Q = \mathbf{0} \}|$$

To evaluate S_2 , we first choose j positions out of k , the number of choices is $\binom{k}{j}$. Without loss of generality we can assume that $\mathbf{x} = (x_1, x_2, \dots, x_k)$, where x_1, x_2, \dots, x_j are nonzero and $x_{j+1} = \dots = x_k = 0$. Then we have

$$\begin{cases} x_1, x_2, \dots, x_j \neq 0 \\ x_1 \mathbf{v}_1 + x_2 \mathbf{v}_2 + \dots + x_j \mathbf{v}_j = \mathbf{0}. \end{cases} \quad (7)$$

Let r be the rank of the matrix with rows $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_j$.

If $r = 1$, then for $1 \leq i \leq j$, $\mathbf{v}_i = t_i \mathbf{v}_j$ for some $t_i \in F_q^*$. Denote by n_j the number of solutions of (7). For arbitrary nonzero elements x_1, x_2, \dots, x_{j-1} ,

- if $x_1 t_1 + x_2 t_2 + \dots + x_{j-1} t_{j-1} = 0$, then $(x_1, x_2, \dots, x_{j-1})$ contributes 1 to n_{j-1} .
- if $x_1 t_1 + x_2 t_2 + \dots + x_{j-1} t_{j-1} \neq 0$, then

$$x_j = -x_1 t_1 - x_2 t_2 - \dots - x_{j-1} t_{j-1}$$

and $(x_1, x_2, \dots, x_{j-1}, x_j)$ contributes 1 to n_j .

Therefore we have $n_{j-1} + n_j = (q-1)^{j-1}$. This recurrence relation and the first term $n_1 = 0$ imply that

$$n_j = \frac{1}{q} ((q-1)^j + (-1)^j (q-1)). \quad (8)$$

If $r \geq 2$, then we may assume that \mathbf{v}_1 and \mathbf{v}_2 are linearly independent. For any fixed nonzero elements x_3, \dots, x_j , the equation

$$x_1 \mathbf{v}_1 + x_2 \mathbf{v}_2 = -x_3 \mathbf{v}_3 - \dots - x_j \mathbf{v}_j$$

has at most one solution. Therefore the number of solutions of (7) is at most $(q-1)^{j-2}$ which is less than (8) except when $q = 2$, j is odd, and

$$\mathbf{v}_1 + \mathbf{v}_2 + \dots + \mathbf{v}_j = \mathbf{0}.$$

In this exceptional case, $n_j = 0 < 1 = (q-1)^{j-2}$ and at least one of \mathbf{v}_i has Hamming weight at least 2 (since an odd number of binary vectors of weight 1 can not have sum $\mathbf{0}$). We may assume $w(\mathbf{v}_j) \geq 2$. Choose $\mathbf{x} = (1, 1, \dots, 1, 0)$. Then $w(\mathbf{x}) = j-1$ and

$$\mathbf{x}Q = \mathbf{v}_1 + \mathbf{v}_2 + \dots + \mathbf{v}_{j-1} = \mathbf{v}_j.$$

Hence

$$w(\mathbf{x}G) = w(\mathbf{x}) + w(\mathbf{v}_j) \geq j-1+2 = j+1.$$

Therefore, in the exceptional case,

$$S_1 < \sum_{i=1}^{j-1} \binom{k}{i} (q-1)^i.$$

In total, by (6) we obtain

$$\begin{aligned} \sum_{i=2}^j A_i(C) &\leq \sum_{i=1}^{j-1} \binom{k}{i} (q-1)^i \\ &\quad + \frac{1}{q} \binom{k}{j} ((q-1)^j + (-1)^j (q-1)) \\ &= \sum_{i=2}^j A_i(E_{n,k,\mathbf{v}}) \end{aligned} \quad (9)$$

for $j \geq 2$ by (5).

By Lemma 2 we get that $A_C(z)$ takes the maximal value for any $z \in (0, 1)$ if and only if C is (equivalent to) $E_{n,k,\mathbf{v}}$. ■

ON AN OLDER BOUND

A special case of [1, Theorem 2.51] is equivalent to the statement that

$$A_C(z) \leq g(z) \stackrel{\text{def}}{=} (1 + (q-1)z)^k + k(q-1)(z^2 - z) \quad (10)$$

for all $[n, k, 2; q]$ codes and all $z \in [0, 1]$. A simple proof goes as follows: we have

$$w(\mathbf{x}G) \geq w(\mathbf{x})$$

for all $\mathbf{x} \in F^k$. Moreover, if $w(\mathbf{x}) = 1$, then $w(\mathbf{x}G) \geq 2$. Hence

$$\begin{aligned} A_C(z) &\leq \sum_{i=0}^k \binom{k}{i} ((q-1)z)^i - k(q-1)z + k(q-1)z^2 \\ &= (1 + (q-1)z)^k + k(q-1)(z^2 - z). \end{aligned}$$

Since (4) is best possible for codes with minimum distance 2, it is clearly at least as good as (10).

If $k = 0$, then $f(z) = g(z) = 1$. If $k = 1$, then

$$f(z) = g(z) = 1 + (q-1)z^2.$$

If $k = q = 2$, then $f(z) = g(z) = 1 + 3z^2$. We will show that in all other cases, $g(z) > f(z)$.

Theorem 5: For $q \geq 2$ and $k \geq 1$ we have

$$g(z) - f(z) = \frac{q-1}{q}(1-z) \left\{ \sum_{j=2}^k \binom{k}{j} ((q-1)^j - (-1)^j) z^j \right\}.$$

In particular, $g(z) > f(z)$ for all $z \in (0, 1)$, except when $q = k = 2$ or $k = 1$.

Proof:

$$\begin{aligned} g(z) - f(z) &= \left(1 + (q-1)z\right)^k + k(q-1)(z^2 - z) \\ &\quad - \frac{1}{q} \left(1 + (q-1)z\right)^{k+1} - \frac{q-1}{q}(1-z)^{k+1} \\ &= \frac{1}{q} \left(1 + (q-1)z\right)^k \left\{ q - 1 - (q-1)z \right\} \\ &\quad - k(q-1)z(1-z) - \frac{q-1}{q}(1-z)^{k+1} \\ &= \frac{q-1}{q}(1-z) \left\{ \left(1 + (q-1)z\right)^k - (1-z)^k - kqz \right\} \\ &= \frac{q-1}{q}(1-z) \left\{ \sum_{j=0}^k \binom{k}{j} ((q-1)^j - (-1)^j) z^j - kqz \right\} \\ &= \frac{q-1}{q}(1-z) \left\{ \sum_{j=2}^k \binom{k}{j} ((q-1)^j - (-1)^j) z^j \right\}. \end{aligned}$$

In particular, if $q > 2$, then $(q-1)^j - (-1)^j > 0$ for all $j \geq 2$. If $q = 2$, $(q-1)^j - (-1)^j > 0$ if j is odd. Hence, $g(z) > f(z)$, except when $k = q = 2$ or $k = 1$. ■

ACKNOWLEDGEMENT

This work is supported by the Norwegian Research Council under the grant 191104/V30. The research of Jinquan Luo is also supported by NSF of China under grant 60903036, NSF of Jiangsu Province under grant 2009182 and the open research fund of National Mobile Communications Research Laboratory, Southeast University (No. 2010D12).

REFERENCES

- [1] T. Kløve, Codes for error detection, World Scientific 2007.